BLUETEAMERS
DEFEND. DETECT. RESPOND.

SOC ANALYST L1 & L2

SCENARIO-BASED INTERVIEW QUESTIONS

15

REAL-WORLD SOC INVESTIGATION SCENARIOS

MASTER PRACTICAL THINKING, NOT MEMORIZED ANSWERS

★ INTERVIEW PREPARATION WORKBOOK ★

PREPARED BY BLUETEAMERS | @BLUETEAMERS_ | BLUETEAMERS.IO

BLUETEAMERS
DEFEND. DETECT. RESPOND.

Impossible Travel Login

SCENARIO

An employee logged in from Hyderabad at 9:02 AM. Five minutes later another successful login happened from Germany. Both logins used the correct password.

INTERVIEW QUESTION

What would you investigate first?

THINK LIKE A SOC ANALYST

Unusual login location within a short time is a strong indicator of compromised credentials or account misuse.

INVESTIGATION – STEP BY STEP

1. **Verify the login events**
   Check authentication logs for both login attempts — time, location, and device.
2. **Check for Impossible Travel**
   Compare the two locations and the time gap. If the user cannot be in both places within the time mentioned, it is impossible travel.
3. **Investigate user risk**
   Check if the account used MFA (Multi-Factor Authentication). If not, the risk is higher.
4. **Take containment actions**
   If compromise is suspected, reset the user's credentials, enable MFA, and monitor for further suspicious activity.

KEY EXPLANATION

- **Impossible Travel:** When a user's account is accessed from two or more locations that are geographically impossible within a short time.
- **MFA (Multi-Factor Authentication):** An extra layer of security beyond username and password.
- **Identity Investigation:** The process of verifying whether an account is legitimately accessed or compromised.

KEY TAKEAWAY

Always validate authentication anomalies. Impossible travel is a strong indicator of credential compromise.

Scenario 02

BLUETEAMERS
DEFEND. DETECT. RESPOND.

PowerShell Download

SCENARIO

Microsoft Defender generated an alert. PowerShell downloaded a file from an unknown website and executed it. No user reported anything.

INTERVIEW QUESTION

What should your first investigation steps be?

THINK LIKE A SOC ANALYST

PowerShell is a powerful built-in Windows tool. Attackers often abuse it to download and run malicious files without installing any external software.

INVESTIGATION – STEP BY STEP

1. **Review the Alert Details**
   Check the alert time, host name, user, PowerShell command, and file URL.
2. **Analyze the PowerShell Command**
   Look for encoded commands, suspicious parameters like Invoke-WebRequest, IEX, -EncodedCommand, or downloads from unknown domains.
3. **Check the Parent Process**
   Identify which process started PowerShell (e.g., cmd.exe, wscript.exe, winword.exe). This shows the execution chain.
4. **Inspect the Downloaded File**
   Check the file path, type, size and calculate the file hash. Analyze it in threat intelligence tools or a sandbox if available.
5. **Check Network Connections**
   Look for connections to external IP addresses or malicious domains around the same time.
6. **Correlate Logs and Escalate**
   Review Defender, EDR, proxy, DNS and firewall logs. If malicious, isolate the endpoint and escalate to L2 / Incident Responder.

KEY EXPLANATION

- **PowerShell:** A legitimate Windows command-line tool widely used for system administration.
- **Living Off The Land (LOTL):** Attackers use built-in system tools like PowerShell to perform malicious activities without installing new software, avoiding detection.
- **Parent Process:** The process that starts another process. It helps us understand how a malicious activity began.
- **Execution:** Running a file, script or command on a system. It is one of the key stages in most cyberattacks.

KEY TAKEAWAY

Always analyze the full execution chain. PowerShell activity should never be ignored, especially when it downloads and executes files from unknown sources.

Scenario 03

BLUETEAMERS
DEFEND. DETECT. RESPOND.

Large Outbound Data Transfer

SCENARIO

At 2 AM, a finance laptop uploaded 18 GB of data to Dropbox.
Normally this user uploads less than 50 MB daily.

INTERVIEW QUESTION

How would you determine whether this is data exfiltration or legitimate activity?

THINK LIKE A SOC ANALYST

Large data transfers at unusual times can be a strong indicator of data exfiltration.
Always validate the user, the data and the destination.

INVESTIGATION – STEP BY STEP

1. **Review the Alert Details**
   Check the alert time, device, user, destination (Dropbox), amount of data transferred and file type (if available).
2. **Validate the User**
   Confirm with the user if the transfer was authorized.
   Check if any business requirement exists.
3. **Analyze User Behavior**
   Compare with the user's normal pattern.
   Check historical upload size, frequency and timing.
4. **Check the Data**
   Identify what type of data was transferred.
   Sensitive data (financial, HR, customer data) is high risk.
5. **Verify the Destination**
   Ensure the Dropbox account is approved and corporate.
   Check if the domain/IP is associated with Dropbox.
6. **Check Access Method**
   Was the transfer done using official Dropbox app, web or API?
   Verify any third-party apps or suspicious tools.
7. **Review Related Logs**
   Check proxy, firewall, SIEM, EDR and DLP logs for more context.
   Look for any other data transfer around the same time.
8. **Determine and Escalate**
   If suspicious, escalate to L2/IR team and consider data containment.
   If legitimate, document and close the alert.

KEY EXPLANATION

- **Outbound Transfer:**
  Data moving from your organization's network to an external location such as Dropbox, Google Drive, OneDrive or another server.
- **Data Exfiltration:**
  Unauthorized transfer of data from a system or network to an external destination, usually to steal sensitive information.
- **Baseline:**
  The normal behavior pattern of a user or system. It includes usual activity like login times, file access and data transfer amount.

KEY TAKEAWAY

Not every large transfer is an attack.
Validate the user, the data, the destination and the context before taking action.
Context + Baseline = Accurate Decision.

INVESTIGATION FLOW

Alert Triggered → Validate User → Analyze User Behavior → Check Data → Verify Destination → Review Logs → Determine & Escalate

Scenario 04

BLUETEAMERS
DEFEND. DETECT. RESPOND.

Multiple Failed Logins

SCENARIO

A server generated 600 failed login attempts
from one IP address.
One login eventually succeeded.

INTERVIEW QUESTION

What attack could this indicate?
How would you investigate?

THINK LIKE A SOC ANALYST

Many failed logins followed by a successful login usually indicates an attack trying to guess or spray passwords.
Focus on validating the successful login.

INVESTIGATION – STEP BY STEP

1. **Review the Alert**
   Check the time, source IP, target account, and the number of failed attempts.
2. **Identify the Attack Type**
   Determine if it is Brute Force or Password Spraying based on patterns and the number of accounts tried.
3. **Check the Successful Login**
   Review the time of the successful login.
   Check the account that was used and login source.
4. **Validate the Source IP**
   Check the IP reputation using threat intelligence.
   See if it is a known malicious IP or proxy.
5. **Review the User Activity**
   Check what actions were performed after the successful login.
   Look for privilege escalation or data access.
6. **Check Related Logs**
   Review firewall, proxy, VPN, EDR and authentication logs around the same time.
7. **Contain if Needed**
   If malicious, block the IP and force password reset.
   Enable MFA if not already enabled.
8. **Escalate and Document**
   Escalate to L2/IR team if suspicious.
   Document all findings and actions.

KEY EXPLANATION

- **Brute Force Attack:**
  An attacker tries many possible passwords for one account until the correct password is found.
- **Password Spraying:**
  An attacker tries a few commonly used passwords across many accounts to avoid account lockout.
- **Successful Authentication:**
  When the attacker finally guesses the correct password and gets access.
- **Account Lockout:**
  A security feature that locks an account temporarily after multiple failed login attempts.

KEY TAKEAWAY

Do not ignore failed logins.
Look for the story behind the alert.
Focus on the successful login and what happened after that.
Validate, correlate and respond.
That's how real threats are caught.

INVESTIGATION FLOW

Alert Triggered → Review Alert Details → Identify Attack Type → Check Successful Login → Validate Source IP → Review User Activity → Contain If Needed → Escalate & Document

BLUETEAMERS
DEFEND. DETECT. RESPOND.

Suspicious Scheduled Task

SCENARIO

An endpoint created a scheduled task that launches PowerShell every morning.
The employee says they never created it.

INTERVIEW QUESTION

What should you investigate?
How would you validate if this is malicious?

THINK LIKE A SOC ANALYST

Scheduled tasks are commonly used by attackers to maintain persistence and execute malicious commands automatically.
Always validate the task, its origin, trigger, and the actions it performs.

INVESTIGATION – STEP BY STEP

1. **Review the Alert Details**
   Check the device, user, task name, time of creation, and the command configured in the task.
2. **Check the Task in Task Scheduler**
   Open Task Scheduler and review the task properties (trigger, action, condition, settings, and history).
3. **Validate the Author and Source**
   Check who created the task and from which account. Verify if it is a legitimate system or admin account.
4. **Analyze the Action**
   Review the command or script executed by the task. Look for PowerShell, cmd.exe, or encoded commands.
5. **Check the Task Trigger**
   Identify when and how often the task runs (e.g., daily, at logon, at startup).
6. **Check the Task Path and Location**
   Verify the folder location of the task. Malicious tasks are often placed in unusual paths.
7. **Review Related Artifacts**
   Check process execution logs, PowerShell logs, file modifications, and registry changes.
8. **Determine and Escalate**
   If malicious, isolate the endpoint and escalate to L2/IR team. If benign, document findings and close the alert.

KEY EXPLANATION

- **Persistence:**
  A technique used by attackers to maintain access to a system even after a reboot or user logout.
- **Scheduled Task:**
  A Windows feature that allows a program or script to run automatically at a specified time or event.
- **PowerShell:**
  A Windows scripting tool often abused by attackers to run commands and bypass security controls.
- **Trigger:**
  Defines when the task will run (e.g., daily, at startup, at logon, or on specific event).
- **Action:**
  The program, script, or command executed by the task.

KEY TAKEAWAY

Attackers love automation. Always check scheduled tasks because they provide a quiet and persistent way to maintain access. Validate everything — don't trust the task just because it looks normal.

INVESTIGATION FLOW

Alert Triggered → Check Task in Task Scheduler → Validate Author and Source → Analyze Action (Command/Script) → Check Trigger and Path → Review Related Artifacts → Determine & Escalate

Scenario 06

BLUETEAMERS
DEFEND. DETECT. RESPOND.

Office Document Spawned CMD

INTERMEDIATE

SCENARIO

A user opened a Microsoft Word document.
Within a few seconds, WINWORD.EXE spawned CMD.EXE which then executed PowerShell.
No user reported any issue.

INTERVIEW QUESTION

What could be happening?
How would you investigate this?

THINK LIKE A SOC ANALYST

Office documents are a common attack vector.
Attackers use macros or exploits to execute commands and gain access.
Focus on the process chain, command execution, network activity and persistence.

INVESTIGATION – STEP BY STEP

1. **Review the Alert**
   Check alert details: time, device, user, process names, command line and any associated IDs.
2. **Check the Process Chain**
   Verify if WINWORD.EXE spawned CMD.EXE and then PowerShell.
   Use EDR or Sysmon process tree.
3. **Analyze the Document**
   Check the file path, hash, and source of the Word file.
   Scan the file in sandbox or VT for malware or macros.
4. **Review Command Execution**
   Check the full command line of CMD and PowerShell.
   Look for encoded commands, script downloads, or suspicious parameters.
5. **Check Network Activity**
   Look for outbound connections made by the process.
   Identify suspicious IPs, domains or unusual destinations.
6. **Check for Persistence**
   Verify if any scheduled task, registry run key, or new service was created.
7. **Review Related Logs**
   Check Windows Event Logs, PowerShell logs, Defender logs, proxy logs and DNS logs.
8. **Determine and Escalate**
   If malicious, isolate the endpoint and escalate to L2/IR.
   If benign, document findings and close the alert.

KEY TERMS EXPLAINED

- **Macro:** A set of instructions in Office documents that can automate tasks. Attackers abuse macros to run malicious code.
- **Process Spawn:** When one program starts another program.
- **PowerShell:** Windows scripting language that attackers use to run commands and bypass security controls.
- **Encoded Command:** Commands are hidden (encoded) to avoid detection.

COMMON INTERVIEW MISTAKE

- ✗ Immediately calling it malware.
- ✓ Always verify the process chain.
- ✓ Analyze the command and context.
- ✓ Validate network and file reputation.

WHAT L1 SHOULD DO

- Validate the alert.
- Collect relevant logs.
- Verify user and activity.
- Escalate if suspicious.

WHAT L2 SHOULD DO

- Deep dive into the root cause.
- Hunt for IOCs across environment.
- Analyze malware or scripts.
- Take response and containment actions.

COMMON LOGS TO CHECK

- Windows Security Event Logs
- Sysmon Logs (Event ID 1, 3, 7)
- PowerShell Operational Logs
- Microsoft Defender Logs
- Proxy / Firewall Logs
- DNS Logs
- EDR Alerts

MITRE ATT&CK MAPPING

Initial Access	T1204	(User Execution)
Execution	T1059	(Command and Scripting Interpreter)
Defense Evasion	T1218	(Signed Binary Proxy Execution)
Persistence	T1547	(Boot or Logon Autostart Execution)
Command & Control	T1071	(Application Layer Protocol)
Discovery	T1082	(System Information Discovery)

USEFUL COMMANDS

```
# Process Tree
Get-Process -IncludeUserName |
Where-Object {$_.Name -in "WINWORD","cmd","powershell"} |
Select-Object Name,Id,Parent,Path

# Check Running Tasks
schtasks /query /fo LIST /v

# Check Network Connections
netstat -ano
```

KEY TAKEAWAY

Office documents can be weaponized. Always analyze the process chain, the command executed, network activity and persistence. Context is everything.

Scenario 07

BLUETEAMERS
DEFEND. DETECT. RESPOND.

Antivirus Disabled

INTERMEDIATE

SCENARIO

Windows Defender was turned off on a workstation by a standard user.
The change occurred outside of normal IT process.
No approved change request was found.

INTERVIEW QUESTION

Why is this a security risk? How would you investigate and respond to this activity?

THINK LIKE A SOC ANALYST

Disabling antivirus can be a strong indicator of malicious activity.
Attackers do this to avoid detection while running payloads, downloading tools or maintaining persistence.
Always validate the user, process and timing.

INCIDENT TIMELINE

- **08:44:12** — **User login**
  User john.doe logged in to the workstation.
- **08:45:01** — **Defender Tampered**
  Real-time protection was turned off.
- **08:45:02** — **Settings Modified**
  Tamper Protection disabled.
- **08:45:10** — **Command Executed**
  PowerShell command executed to disable Defender.
- **08:45:30** — **Suspicious Download**
  A file was downloaded from the internet.
- **08:46:02** — **Process Execution**
  Suspicious process executed from user temp directory.
- **08:47:15** — **Outbound Connection**
  Connection established to external IP.
- **08:48:20** — **SOC Alert Generated**
  Defender disable alert triggered.

WHAT SHOULD THE ANALYST INVESTIGATE?

- Who disabled the antivirus and why?
- What process or command was used?
- What happened before and after the event?
- Any suspicious downloads, executions or connections?
- Is the endpoint compromised?

INVESTIGATION – STEP BY STEP

1. **Review the Alert**
   Check alert details: time, device, user, process name and event id.
2. **Check the User**
   Validate user role and confirm if the action was authorized.
3. **Review Event Logs**
   Check Windows Security Event Logs for event IDs: 5007, 5010, 5012.
4. **Analyze the Process**
   What process/command was used to disable Defender? (e.g., PowerShell, REG, CMD)
5. **Check for Related Activities**
   Look for suspicious files, scripts, scheduled tasks, registry changes, downloads and executions.
6. **Review Network Activity**
   Check for any outbound connections after Defender was disabled.
7. **Check for Persistence**
   Look for any persistence mechanisms.
8. **Contain and Escalate**
   If malicious, isolate the endpoint and escalate to L2/IR team.

COMMON LOGS TO CHECK

- Windows Security Event Logs (5007, 5010, 5012)
- PowerShell Operational Logs
- Microsoft Defender Logs
- Sysmon Logs (Event ID 1, 7, 11)
- EDR Alerts
- Proxy / Firewall Logs
- DNS Logs

MITRE ATT&CK MAPPING

Defense Evasion	T1562.001	Impair Defenses: Disable or Modify Tools
Execution	T1059	Command and Scripting Interpreter
Persistence	T1547.001	Boot or Logon Autostart: Registry Run Keys
Discovery	T1082	System Information Discovery
Command & Control	T1071	Application Layer Protocol

USEFUL COMMANDS

```
# Check Defender status
Get-MpComputerStatus

# Check who disabled Defender
Get-WinEvent -LogName "Microsoft-Windows-Windows Defender/Operational" | Where-Object {$_.Id -eq 5007}

# Check recent changes
Get-WinEvent -LogName Security | Where-Object {$_.Id -in 5007,5010,5012}

# Check running processes
Get-Process | Sort-Object CPU -Descending
```

COMMON INTERVIEW MISTAKE

- ✗ Assuming every Defender disable is an attack.
- ✗ Not checking who performed the action.
- ✗ Ignoring what happened before and after.
- ✗ Not looking at related logs and network activity.

INTERVIEWER'S EXPECTATION

- ✓ You verify the evidence.
- ✓ You correlate multiple data points.
- ✓ You understand attacker behavior.
- ✓ You follow a structured approach.

KEY TAKEAWAY

Attackers disable security controls to operate freely. Always investigate the who, when, how and what's next. Context is everything.

Scenario 08

BLUETEAMERS
DEFEND. DETECT. RESPOND.

Beaconing Traffic

INTERMEDIATE

SCENARIO

Network monitoring detected a workstation making small outbound connections to an unknown external IP every 60 seconds.
The traffic is consistent and ongoing.
No user activity is associated with it.

INTERVIEW QUESTION

What does this indicate? How would you investigate this scenario?

THINK LIKE A SOC ANALYST

Beaconing is commonly used by malware or compromised hosts to maintain communication with a C2 (Command & Control) server.
It is designed to be stealthy, low and slow to avoid detection.
Focus on patterns, frequency, destination and context.

BEACONING TRAFFIC TIMELINE (EXAMPLE)

10:15:01	**Workstation starts**	Normal user login.
10:15:30	**First outbound connection**	Small packet to 203.0.113.45:443
10:16:30	**Outbound connection**	Similar packet size and destination.
10:17:30	**Outbound connection**	Pattern continues every 60 seconds.
10:25:00	**Analyst Alert**	Beaconing behavior detected.
10:25:30	**SOC Alert Generated**	Beaconing traffic alert triggered.

WHAT SHOULD THE ANALYST INVESTIGATE?

- What process is generating the traffic?
- What is the destination IP / domain reputation?
- Is the traffic encrypted (HTTPS, TLS, or custom)?
- What is the pattern, frequency and data size?
- Any related processes, files or persistence mechanisms?
- Is the host communicating with known C2 infrastructure?
- Has any lateral movement or data exfiltration occurred?

INVESTIGATION – STEP BY STEP

1. **Review the Alert**
   Check alert details: time, device, user, src/dest IP, port, protocol and bytes transferred.
2. **Identify the Process**
   Find the process generating the outbound connections using EDR / NetFlow / Sysmon.
3. **Analyze Network Pattern**
   Check frequency, packet size, duration and consistency of connections.
4. **Check Destination Reputation**
   Validate IP/domain using threat intelligence (VirusTotal, AbuseIPDB, ThreatFox, etc.).
5. **Inspect Traffic Details**
   Check protocol (HTTP/S, DNS, TCP, ICMP), headers, SNI, User-Agent and certificates.
6. **Check for Malware Indicators**
   Review file hash, script execution, registry changes and persistence mechanisms.
7. **Review Related Logs**
   Check firewall, proxy, DNS, EDR and Windows event logs for more context.
8. **Contain and Escalate**
   If malicious, isolate the host, block the indicators and escalate to L2/IR team.

COMMON LOGS TO CHECK

- Firewall Logs
- NetFlow / Zeek Logs
- DNS Logs
- Proxy Logs
- EDR / XDR Alerts
- Windows Event Logs (Security, Sysmon)
- Suricata / IDS Logs

MITRE ATT&CK MAPPING

Command & Control	T1071	Application Layer Protocol
Command & Control	T1090	Proxy
Command & Control	T1105	Ingress Tool Transfer
Command & Control	T1071.001	Web Protocols
Discovery	T1049	System Network Connections
Defense Evasion	T1027	Obfuscated Files or Information

USEFUL COMMANDS

```
# Check network connections
netstat -ano | findstr ESTABLISHED

# Get process details
tasklist /FI "PID eq <PID>" /V

# Check DNS queries
nslookup <domain>

# Reputation check
curl -s https://www.virustotal.com/api/v3/ip/<IP>
  | jq '.data.attributes.last_analysis_stats'
```

COMMON INTERVIEW MISTAKE

- ✗ Ignoring traffic because it is low and slow.
- ✗ Not validating the process responsible.
- ✗ Not checking destination reputation.
- ✗ Not correlating logs.

WHAT L1 SHOULD DO

- ✓ Validate the alert.
- ✓ Identify the process.
- ✓ Check destination IP/domain.
- ✓ Collect logs and context.
- ✓ Escalate if suspicious.

WHAT L2 SHOULD DO

- ✓ Deep dive investigation.
- ✓ Malware / payload analysis.
- ✓ Hunt for IOCs across environment.
- ✓ Containment and eradication.
- ✓ Document and report.

KEY TAKEAWAY

Beaconing is designed to be stealthy. Patterns don't lie. Always analyze process, network behavior and context together.

Scenario 09

BLUETEAMERS
DEFEND. DETECT. RESPOND.

Unusual File Access

INTERMEDIATE

SCENARIO

A user account accessed sensitive HR files
that are not part of their normal job role.
The access happened outside of working hours.
No business justification was found.

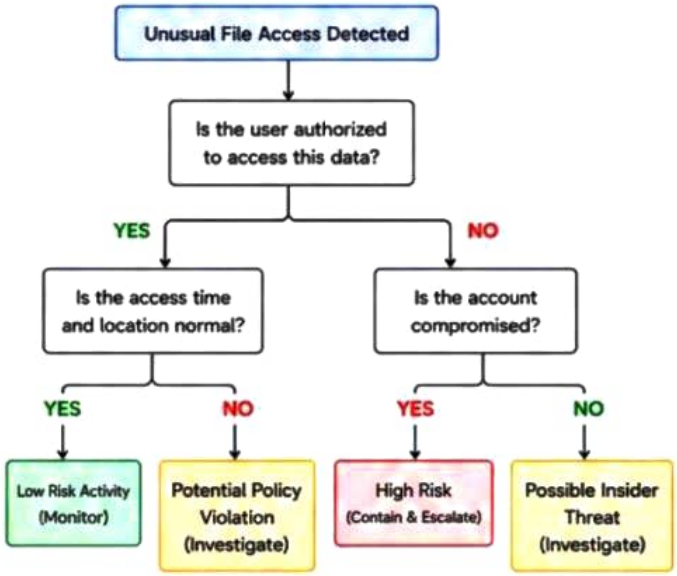
INTERVIEW QUESTION

**What could be the cause of this activity?
How would you investigate and
respond to this alert?**

THINK LIKE A SOC ANALYST

Unusual file access can be caused by insider threat, credential compromise,
lateral movement or data exfiltration attempts.
Focus on the user, the data accessed, the time, and what happened next.
Context is the key to understanding intent.

UNUSUAL FILE ACCESS – DECISION TREE



CHECK CONTEXT

- File Sensitivity
- Access Volume
- Time & Location
- User Behavior
- Data Movement After Access

INVESTIGATION – STEP BY STEP

1. **Review the Alert**
   Check alert details: user, device, file path, time, and type of access.
2. **Validate User and Role**
   Confirm the user's role and whether they should have access to the file.
3. **Review Access Logs**
   Check file access logs, Windows Security Event Logs (4663, 4656), and file server logs.
4. **Analyze Access Pattern**
   Check the time, duration, number of files accessed and whether it's unusual for the user.
5. **Check Source and Location**
   Verify the device, IP address, and location of the access.
6. **Look for Data Movement**
   Check if the files were copied, downloaded, emailed, compressed or moved.
7. **Check for Related Activity**
   Look for logon anomalies, privilege escalation, process execution and network connections.
8. **Contain and Escalate**
   If malicious or suspicious, isolate the account/host and escalate to L2/IR team.

COMMON LOGS TO CHECK

- Windows Security Event Logs (4663, 4656, 4624, 4672)
- File Server / NAS Logs
- EDR / XDR Alerts
- DLP Logs
- VPN / Proxy Logs
- Firewall Logs
- Email Logs

MITRE ATT&CK MAPPING

Initial Access	T1078	Valid Accounts
Execution	T1059	Command and Scripting Interpreter
Discovery	T1083	File and Directory Discovery
Collection	T1005	Data from Local System
Exfiltration	T1041	Exfiltration Over C2 Channel
Impact	T1485	Data Destruction

USEFUL COMMANDS

```
# Check file access events
wevtutil qe Security /q:"[System[(EventID=4663)
or (EventID=4656)]]" /f:text /c:20

# Check logged on sessions
query user

# Check recent files accessed
powershell "Get-ChildItem $env:USERPROFILE\Recent"

# Check file server shares
net share
```

COMMON INTERVIEW MISTAKE

- ✗ Assuming it is always malicious.
- ✗ Ignoring context (role, time, business need).
- ✗ Not checking what happened after the access.
- ✗ Not correlating logs and user behavior.

WHAT L1 SHOULD DO

- ✓ Validate the alert.
- ✓ Collect and review relevant logs.
- ✓ Verify user role and access justification.
- ✓ Escalate if suspicious.

WHAT L2 SHOULD DO

- ✓ Deep dive into root cause.
- ✓ Hunt for attacker persistence.
- ✓ Check for data exfiltration.
- ✓ Document and report findings.

KEY TAKEAWAY

Not every access is malicious, but every unusual access deserves attention.
Validate, correlate and understand the story behind the alert.

Scenario 10

BLUETEAMERS
DEFEND. DETECT. RESPOND.

Encoded PowerShell

INTERMEDIATE

SCENARIO

A PowerShell command was executed with -EncodedCommand parameter.
The command is obfuscated and not readable in the logs.
No user reported this activity.

INTERVIEW QUESTION

What could be the attacker trying to do? How would you decode and investigate this command?

THINK LIKE A SOC ANALYST

Attackers encode PowerShell commands to bypass detections and hide their intent.
They may download payloads, run scripts, steal data or maintain persistence.
Decode the command, understand the intent, and investigate the full execution chain.

INVESTIGATION – STEP BY STEP

1. **Review the Alert**
   Check alert details: time, device, user, process name, command line and related IDs.
2. **Identify the Encoded Command**
   Look for "-EncodedCommand" or "-enc" in the command line or PowerShell logs.
3. **Decode the Command**
   Copy the encoded string and decode it from Base64 to readable format.
4. **Analyze the Decoded Command**
   Understand what the command is doing (download, execute, connect, modify registry, etc.).
5. **Check the Process Chain**
   Review parent process, child process and command lineage using EDR / Sysmon.
6. **Check for Network Activity**
   Look for any outbound connections triggered by the decoded command.
7. **Check for Indicators of Compromise**
   Look for files created, registry changes, scheduled tasks, or persistence mechanisms.
8. **Contain and Escalate**
   If malicious, isolate the endpoint and escalate to L2/IR team.

DECODED COMMAND EXAMPLE

Original (Encoded):

```
powershell -enc SQBFAFgAVwAgACgARwBlAHQtAC0AQwBvAG0A
AGIAaQBuAGEAdAB2pAG8AbgApAA==
```

Decoded (Readable):

```
IEX (Get-Combination)
```

HOW TO DECODE (BASE64)

PowerShell Command:

```
[Text.Encoding]::UTF8.GetString([Convert]::FromBase64String(
"SQBFAFgAVwAgACgARwBlAHQtAC0AQwBvAG0AAGIAaQBuAGEA
AdABpAG8AbgApAA=="))
```

Online Tools:

- cyberchef.org
- base64decode.org
- dotnetfiddle.net

COMMON ATTACK INTENTS

- Download and execute payloads
- Establish reverse shell
- Credential dumping
- Data exfiltration
- Persistence mechanism

COMMON LOGS TO CHECK

- Windows Security Event Logs (4688, 4104)
- PowerShell Operational Logs
- Sysmon Logs (Event ID 1, 7, 11)
- EDR / XDR Alerts
- Firewall / Proxy Logs
- DNS Logs
- File / Registry Monitoring Logs

MITRE ATT&CK MAPPING

Execution	>	T1059.001	PowerShell
Command & Control	>	T1071	Application Layer Protocol
Defense Evasion	>	T1027	Obfuscated/Compressed Files
Persistence	>	T1547.001	Boot or Logon Autostart
Discovery	>	T1082	System Information Discovery
Collection	>	T1005	Data from Local System
Exfiltration	>	T1041	Exfiltration Over C2 Channel

USEFUL COMMANDS

```
# Check PowerShell logs
Get-WinEvent -LogName "Microsoft-Windows-PowerShell/
Operational" | Where-Object {$_.Id -eq 4104}

# Get process details
Get-Process -Id <PID> | Select-Object Id,ProcessName,
Path,StartTime

# Check network connections
netstat -ano | findstr ESTABLISHED

# Decode Base64 in PowerShell
[Text.Encoding]::UTF8.GetString(
[Convert]::FromBase64String("<ENCODED_STRING>"))
```

COMMON INTERVIEW MISTAKE

- ✗ Not decoding the command.
- ✗ Assuming every encoded command is malicious.
- ✗ Ignoring process chain and context.
- ✗ Not checking network and persistence.

WHAT L1 SHOULD DO

- ✓ Validate the alert.
- ✓ Decode the command.
- ✓ Collect logs and context.
- ✓ Check user and process activity.
- ✓ Escalate if suspicious.

WHAT L2 SHOULD DO

- ✓ Deep dive into command intent.
- ✓ Hunt for attacker tools and IOCs.
- ✓ Analyze payloads and scripts.
- ✓ Contain, eradicate and strengthen detections.

KEY TAKEAWAY

Encoded PowerShell is a red flag. Decoding and understanding the command is essential to uncover the attacker's real intent. Context is everything.

Scenario 11

BLUETEAMERS
DEFEND. DETECT. RESPOND.

Suspicious RDP Login

INTERMEDIATE

SCENARIO

A successful RDP login was detected on a workstation from an unusual external IP at 02:13 AM. The user was not working at that time. No service desk request was found.

INTERVIEW QUESTION

What could be happening? How would you investigate and respond to this activity?

THINK LIKE A SOC ANALYST

RDP logins from unusual locations or times can indicate brute force attacks, credential compromise, insider threat or lateral movement.
Focus on who logged in, from where, using what method and what happened next.

LOGIN TIMELINE (EXAMPLE)

02:13 AM — RDP Login
Successful logon from IP 203.0.113.45 using user john.doe

02:13 AM — Session Established
RDP session created on workstation WIN-10-23 (Internal IP 10.1.5.23)

02:14 AM — Process Created
cmd.exe → powershell.exe started by user

02:15 AM — Network Connection
Outbound connection to 185.199.108.153 (Unknown ASN)

02:17 AM — Suspicious Activity
Files accessed in C:\Users\Public\ and registry modified

02:20 AM — SOC Alert Generated
Suspicious RDP activity detected

INVESTIGATION – STEP BY STEP

1. **Review the Alert**
   Check alert details: time, user, source IP, destination, and method.
2. **Validate the Login**
   Check if the user was expected to login at that time and from that location.
3. **Review RDP Login Events**
   Check Windows Event Logs for successful RDP logons (Event ID 4624 Type 10).
4. **Check IP Reputation**
   Validate source IP using threat intelligence tools (VirusTotal, AbuseIPDB, IPQualityScore).
5. **Analyze User Activity After Login**
   Check processes, commands executed, files accessed and registry changes.
6. **Check for Lateral Movement**
   Look for other system access, admin shares access, remote services or credential dumping.
7. **Review Network Activity**
   Check outbound connections, DNS queries and data transfers after the login.
8. **Contain and Escalate**
   If malicious, reset credentials, isolate the endpoint and escalate to L2/IR team.

WINDOWS EVENT IDs TO CHECK

- 4624 - Successful Logon (Type 10 RDP)
- 4625 - Failed Logon
- 4634 - Logoff
- 4672 - Special Privileges Assigned
- 4778 - RDP Session Reconnected
- 1149 - Remote Desktop Services: User Authentication Succeeded

MITRE ATT&CK MAPPING

Initial Access	T1190	Valid Accounts
Execution	T1059	Command and Scripting Interpreter
Persistence	T1547	Boot or Logon Autostart Execution
Privilege Escalation	T1068	Exploitation for Privilege Escalation
Defense Evasion	T1027	Obfuscated Files or Information
Lateral Movement	T1021	Remote Services
Discovery	T1087	Account Discovery

USEFUL COMMANDS

```
# Check RDP logons
Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4624;Data=@{TargetLogonType=10}} | Format-Table TimeCreated,Id,Message -AutoSize

# Check active RDP sessions
query session

# Check recent logons
whoami /all

# Check network connections
netstat -ano | findstr ESTABLISHED
```

COMMON INTERVIEW MISTAKES

- ✗ Ignoring the source IP and geolocation.
- ✗ Not checking event ID 4624 Type 10.
- ✗ Assuming all RDP logins are malicious.
- ✗ Not reviewing post-login activities.
- ✗ Not correlating with other logs and network activity.

WHAT L1 SHOULD DO

- ✓ Validate the alert.
- ✓ Collect and review relevant logs.
- ✓ Verify user and login context.
- ✓ Check IP reputation.
- ✓ Escalate if activity is suspicious.

WHAT L2 SHOULD DO

- ✓ Deep dive into attacker behavior.
- ✓ Hunt for lateral movement and persistence.
- ✓ Analyze malware or tools used.
- ✓ Contain, eradicate and guide recovery.
- ✓ Document and create IOCs.

KEY TAKEAWAY

Time-based (02:13 AM) and location-based anomalies in RDP logins are strong indicators. Always investigate beyond the login and review what happened next.

Scenario 12

BLUETEAMERS
DEFEND. DETECT. RESPOND.

DNS Tunneling

INTERMEDIATE

SCENARIO

DNS queries to a suspicious domain are detected. Analysis shows DNS tunneling used for data exfiltration or C2 communication.

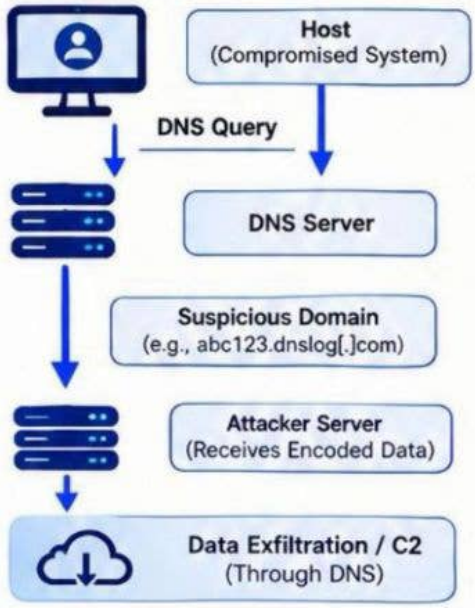
INTERVIEW QUESTION

What is DNS tunneling?
How would you investigate this activity?
What logs and indicators will you check?

THINK LIKE A SOC ANALYST

DNS tunneling lets attackers hide C2 traffic and exfiltrate data inside DNS queries and responses. It appears as unusual DNS traffic with long, encoded subdomains, high query volume and queries to suspicious domains. Your job is to detect, analyze and confirm if DNS is being abused.

DNS TUNNELING – NETWORK FLOW



INVESTIGATION – STEP BY STEP

1. **Review the Alert**
   Check DNS logs for high query volume, unusual domains and long subdomain names.
2. **Analyze DNS Query**
   Look for encoded or random-looking subdomains, frequent queries and DNS tunneling patterns.
3. **Check Related Logs**
   Correlate with firewall, proxy and endpoint logs for C2 activity.
4. **Identify the Source**
   Find the host generating the suspicious DNS traffic.
5. **Assess the Risk**
   Confirm if the traffic is tunneling data to an attacker infrastructure.
6. **Respond**
   Block the domain, isolate the endpoint and escalate to L2 team.

DNS TUNNELING INDICATORS

- ✓ Very long or random subdomain names
- ✓ High volume of DNS queries
- ✓ Queries to dynamic or known malicious domains
- ✓ Large DNS responses (unusually big size)
- ✓ Frequent queries to the same domain

COMMON LOGS TO CHECK

- DNS Logs (Windows / Firewall)
- Proxy Logs
- Network Logs
- EDR Alerts
- Sysmon Logs

MITRE ATT&CK MAPPING

Command & Control → T1071.004 (DNS)

USEFUL COMMANDS

```
# Check DNS queries
nslookup example.com

# View DNS cache
ipconfig /displaydns
```

L1 vs L2

- **L1**: Detect suspicious DNS activity, collect logs, escalate.
- **L2**: Perform deep analysis, find C2, confirm data exfiltration.

KEY TAKEAWAY: DNS tunneling hides malicious activity inside normal DNS traffic. Look for unusual domains, long subdomains and high DNS query volume.

Scenario 13

BLUETEAMERS
DEFEND. DETECT. RESPOND.

New Administrator Account Created

INTERMEDIATE

SCENARIO

A new local administrator account was created on a server that is not part of the standard build process. This account was not created by IT operations.
No change request was found.

INTERVIEW QUESTION

What could be the reason for this activity? How would you investigate and respond to this aLert?

THINK LIKE A SOC ANALYST

Attackers create new admin accounts to maintain persistence, escalate privileges or regain access if their initial access is lost.
Focus on who created the account, why it was created and what was done after creation.

ATTACK FLOW

COMPROMISED ACCOUNT
Attacker gains initial access using phishing, weak password or exploitation

PRIVILEGE ESCALATION
Attacker escalates privileges using vulnerabilities or misconfigurations

ADMIN ACCOUNT CREATED
New administrator account is created for persistence

PERSISTENCE ESTABLISHED
Account is used for future access and lateral movement

FUTURE ACCESS & IMPACT
Attacker maintains control and performs additional malicious activities

WINDOWS EVENT IDS TO CHECK

EVENT ID	EVENT NAME	DESCRIPTION	WHY IT MATTERS
4720	A user account was created	New user account created on the system	Confirms creation of the new admin account
4728	A member was added to a security-enabled global group	Account added to Administrators group	Confirms admin privileges assigned
4732	A member was added to a local group	Account added to local Administrators	Shows local admin privileges granted
4672	Special privileges assigned to new logon	User logged on with special privileges	Indicates admin logon using the account
4624	An account was successfully logged on	Successful logon with the account	Confirms account was used to log on

INVESTIGATION – STEP BY STEP

1. **Review the Alert**
   Check alert details: time, device, account name, source process and user context.
2. **Validate Account Creation**
   Confirm if the account was created by authorized IT personnel or if there is a change request.
3. **Check Windows Event Logs**
   Review relevant Windows Security Events (see table on left) for account creation and privilege assignment.
4. **Analyze Parent Process**
   Identify the process used to create the account (e.g., net user, powershell, mmc.exe).
5. **Check Account Attributes**
   Check if the account is local or domain, disabled/enabled, and group membership.
6. **Review Logon Activity**
   Check if the new account was used to log on locally or remotely after creation.
7. **Look for Persistence Mechanisms**
   Check for scheduled tasks, services, startup items or registry modifications.
8. **Contain and Escalate**
   If malicious, disable the account, reset credentials and escalate to L2/IR team.

COMMON LOGS TO CHECK

- Windows Security Event Logs
- Sysmon Logs (Event ID 1, 10, 11)
- PowerShell Operational Logs
- EDR / XDR Alerts
- Firewall Logs
- Proxy / Web Gateway Logs
- Active Directory Logs

MITRE ATT&CK MAPPING

Initial Access	>	T1078	Valid Accounts
Execution	>	T1059	Command and Scripting Interpreter
Persistence	>	T1547	Boot or Logon Autostart Execution
Privilege Escalation	>	T1068	Exploitation for Privilege Escalation
Defense Evasion	>	T1036	Masquerading
Credential Access	>	T1003	Credential Dumping
Lateral Movement	>	T1021	Remote Services

USEFUL COMMANDS

```
# List local users
net user
-----------------------------------------------------------
# Check local administrators group
net localgroup administrators
-----------------------------------------------------------
# Check recent account creations
Get-WinEvent -FilterHashtable @{LogName='Security';
Id=4720} | Format-Table TimeCreated,Message -AutoSize
-----------------------------------------------------------
# Check group membership changes
Get-WinEvent -FilterHashtable @{LogName='Security';
Id=4728,4732} | Format-Table TimeCreated,Message -AutoSize
```

COMMON INTERVIEW MISTAKES

- ✗ Assuming IT created without verifying.
- ✗ Ignoring group membership events.
- ✗ Not checking logon activity of the new account.
- ✗ Not investigating parent process or execution method.
- ✗ Not correlating with other logs or alerts.

WHAT L1 SHOULD DO

- ✓ Validate the alert.
- ✓ Collect and review relevant logs.
- ✓ Verify account creation and group membership.
- ✓ Check recent logons with the account.
- ✓ Escalate if suspicious.

WHAT L2 SHOULD DO

- ✓ Deep dive into attacker behavior.
- ✓ Correlate with other events and logs.
- ✓ Hunt for related persistence mechanisms.
- ✓ Contain, remove the account and harden the system.
- ✓ Document and create IOCs.

KEY TAKEAWAY

Unauthorized admin accounts are a critical sign of compromise. Always validate the reason, investigate the creation method, review usage and look for persistence.

Scenario 14

Phishing Investigation

BLUETEAMERS
DEFEND. DETECT. RESPOND.

INTERMEDIATE

SCENARIO

A user reported receiving a suspicious email with an urgent request to verify their account.
The user clicked the link and entered their credentials on a fake login page.
We need to investigate the phishing incident.

INTERVIEW QUESTION

What indicators show this is a phishing attempt?
How would you investigate and respond to this incident?

THINK LIKE A SOC ANALYST

Phishing attacks aim to steal credentials, deliver malware or trick users into taking malicious actions.
Focus on email artifacts, URLs, attachments, user behavior and endpoint evidence.
Connect all the dots before concluding.

PHISHING EMAIL EXAMPLE

From: support@micr0soft-security.com
To: john.doe@company.com
Subject: Action Required: Verify Your Account
Date: Tue, 30 Apr 2024 09:18:52 +0000

Microsoft

Action Required!

Dear User,

We detected unusual sign-in activity on your account.
Please verify your account immediately to avoid suspension.

Verify Account Now

https://secure-microsoft-login.com/verify
(hover to see link)

Thank you,
Microsoft Security Team

PHISHING ATTACK FLOW

PHISHING EMAIL DELIVERED → USER CLICKS LINK → FAKE LOGIN PAGE OPENED → CREDENTIALS STOLEN → ATTACKER GAINS ACCESS → SOC ALERT GENERATED

EMAIL ANALYSIS CHECKLIST

- **EMAIL HEADERS** — Check SPF, DKIM, DMARC, sender IP, Reply-To, and Received paths.
- **SUSPICIOUS URLS** — Inspect URL for typos, strange domains, IP addresses or URL shorteners.
- **ATTACHMENTS** — Check file type, hashes and scan in sandbox for malicious behavior.
- **SANDBOX ANALYSIS** — Run attachments/URLs in sandbox and review behavior report.
- **USER INTERVIEW** — Ask user how the email was received, what actions were taken.
- **BROWSER HISTORY** — Check visited URLs, login attempts and saved credentials.
- **ENDPOINT & EMAIL SECURITY LOGS** — Review Defender, Proxy, EDR and Email Gateway logs for related events.

INDICATORS OF PHISHING

- Generic greetings (Dear User, Dear Customer)
- Urgent language or threats of account suspension
- Mismatched or spoofed sender domain
- Suspicious links or shortened URLs
- Spelling / grammar mistakes
- Unexpected attachments
- Requests for sensitive information

COMMON LOGS TO CHECK

- Email Gateway / Security Logs
- Microsoft 365 Defender Logs
- Proxy / Web Gateway Logs
- EDR / XDR Alerts
- DNS Logs
- User Sign-in Logs (Azure AD / AD)

USEFUL COMMANDS

```
# Check email header
Get-MessageTrace -MessageId <MessageId>

# Search email in Microsoft 365 Defender
Search-UnifiedAuditLog -Operations "Send","Deliver"

# Check user sign-in logs
Get-AzureADAuditSignInLogs -UserPrincipalName john.doe@company.com

# Check URL reputation
nslookup domain.com
whois domain.com

# Check process / network connections
netstat -ano  | findstr ESTABLISHED
```

COMMON INTERVIEW MISTAKES

- ✗ Only checking the URL and ignoring headers.
- ✗ Not validating domain / sender reputation.
- ✗ Skipping sandbox analysis.
- ✗ Not reviewing logs after user action.
- ✗ Not correlating with other alerts.

WHAT L1 SHOULD DO

- ✓ Validate the alert.
- ✓ Collect email & header details.
- ✓ Check URLs & attachments.
- ✓ Review logs and user activity.
- ✓ Escalate if malicious.

WHAT L2 SHOULD DO

- ✓ Deep dive into artifacts.
- ✓ Correlate across multiple logs.
- ✓ Identify scope and impact.
- ✓ Create IOCs and blocking rules.
- ✓ Document and report findings.

KEY TAKEAWAY

Phishing is a human + technical attack. A thorough investigation of email artifacts, user actions and logs is essential to prevent future incidents and protect the organization.

Scenario 15

SOC ANALYST INVESTIGATION PLAYBOOK

Full Incident Investigation – From Alert to Closure

BLUETEAMERS
DEFEND. DETECT. RESPOND.

ADVANCED

SCENARIO

One endpoint triggered multiple suspicious activities throughout the day, including PowerShell execution, Defender disabled, beaconing to external IP, scheduled task creation and credential dumping.

INTERVIEW QUESTION

Walk me through how you would investigate this incident from the first alert until the case is closed.

INCIDENT TIMELINE

08:01 AM – User Login
User john.doe logged in to workstation IP 10.1.5.23

08:03 AM – Malicious Document Executed
User opened phishing document invoice.pdf from email

08:04 AM – PowerShell Execution
powershell.exe executed with encoded command

08:05 AM – Payload Downloaded
File downloaded from hxxp://185.199.108.153/payload.exe

08:06 AM – Defender Disabled
Windows Defender real-time protection disabled via PowerShell

08:08 AM – Beaconing to C2
Outbound connection to 185.199.108.153:443 repeated at regular intervals

08:12 AM – Credential Dumping
Mimikatz executed and credentials dumped (lsass.exe access)

08:18 AM – Persistence Established
Scheduled task created for persistence (every 5 minutes)

SOC Alert Generated
Multiple detections triggered – High Severity

INVESTIGATION FLOW

ALERT – Receive Alert → VALIDATE – Confirm Legitimacy → COLLECT – Collect Logs & Data → ANALYZE – Analyze Indicators → CONTAIN – Contain Threat → ESCALATE – Escalate to L2 / IR Team → RECOVER – Recover & Remediate → LESSONS LEARNED – Document & Improve

MITRE ATT&CK MATRIX (Attack Progression)

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Command & Control	Exfiltration
T1566	T1059	T1547	T1068	T1562	T1003	T1087	T1071	T1041

L1 (SOC ANALYST) RESPONSIBILITIES

- Validate the alert and severity
- Collect endpoint, network and user logs
- Identify affected assets and users
- Check IOCs and threat intelligence
- Document all findings and actions
- Escalate to L2 / Incident Response Team

L2 (SENIOR ANALYST / IR) RESPONSIBILITIES

- Perform deep dive analysis and root cause
- Hunt for related activity across environment
- Reverse engineer malware / analyze payload
- Create IOCs and detection rules
- Contain threat and eradicate from environment
- Recommend recovery and hardening steps
- Prepare executive summary and lessons learned

KEY EVIDENCE TO COLLECT

- **Windows Event Logs (Security, System, PowerShell)** – Logon, Process Creation, Script Block, Task Scheduler
- **EDR / Defender Logs** – Alerts, Threat Detections, Mitigation Actions
- **Network Logs** – DNS, Proxy, Firewall, NetFlow, Beaconing
- **Filesystem Artifacts** – Malicious files, Prefetch, Amcache, Jump Lists
- **Memory Artifacts** – Memory dump, LSASS dump
- **Email & User Activity** – Email headers, Clicked URLs, User actions

INDICATORS OF COMPROMISE (IOCs)

- powershell.exe with encoded commands
- Connections to 185.199.108.153
- File downloaded: payload.exe
- Defender disabled via Set-MpPreference
- Mimikatz / lsass.exe access
- Scheduled task: UpdateService
- Unusual parent-child process relationships
- Multiple logons in short time

USEFUL COMMANDS

```
# Get recent PowerShell events
Get-WinEvent -LogName "Microsoft-Windows-PowerShell/Operational" |
Select-Object TimeCreated, Id, Message -First 20

# List scheduled tasks
schtasks /query /fo LIST /v

# Check Defender status
Get-MpComputerStatus | Select-Object AMServiceEnabled,
AntivirusEnabled, RealTimeProtectionEnabled

# Check network connections
netstat -ano | findstr ESTABLISHED

# Check process tree
Get-Process | Sort-Object StartTime | Select-Object
ProcessName, Id, StartTime

# Check recent logons
Get-WinEvent -FilterHashtable @{LogName='Security';
Id=4624} | Select TimeCreated, Message -First 20
```

COMMON INTERVIEW MISTAKES

- ✗ Jumping to conclusions without evidence.
- ✗ Not validating alert with full context.
- ✗ Missing important logs and artifacts.
- ✗ Not checking lateral movement.
- ✗ Skipping threat intelligence validation.
- ✗ Poor documentation and communication.

WHAT L1 SHOULD DO

- ✓ Validate and triage the alert.
- ✓ Collect and preserve logs.
- ✓ Check user and endpoint behavior.
- ✓ Identify quick wins and IOCs.
- ✓ Document everything clearly.
- ✓ Escalate with summary.

WHAT L2 SHOULD DO

- ✓ Deep dive into attacker behavior.
- ✓ Hunt across environment.
- ✓ Correlate all evidence.
- ✓ Create detections & IOCs.
- ✓ Contain, eradicate and recover.
- ✓ Report and improve.

KEY TAKEAWAY

A structured investigation with the right process, tools and mindset helps you catch the full attack chain, reduce impact and prevent future incidents.